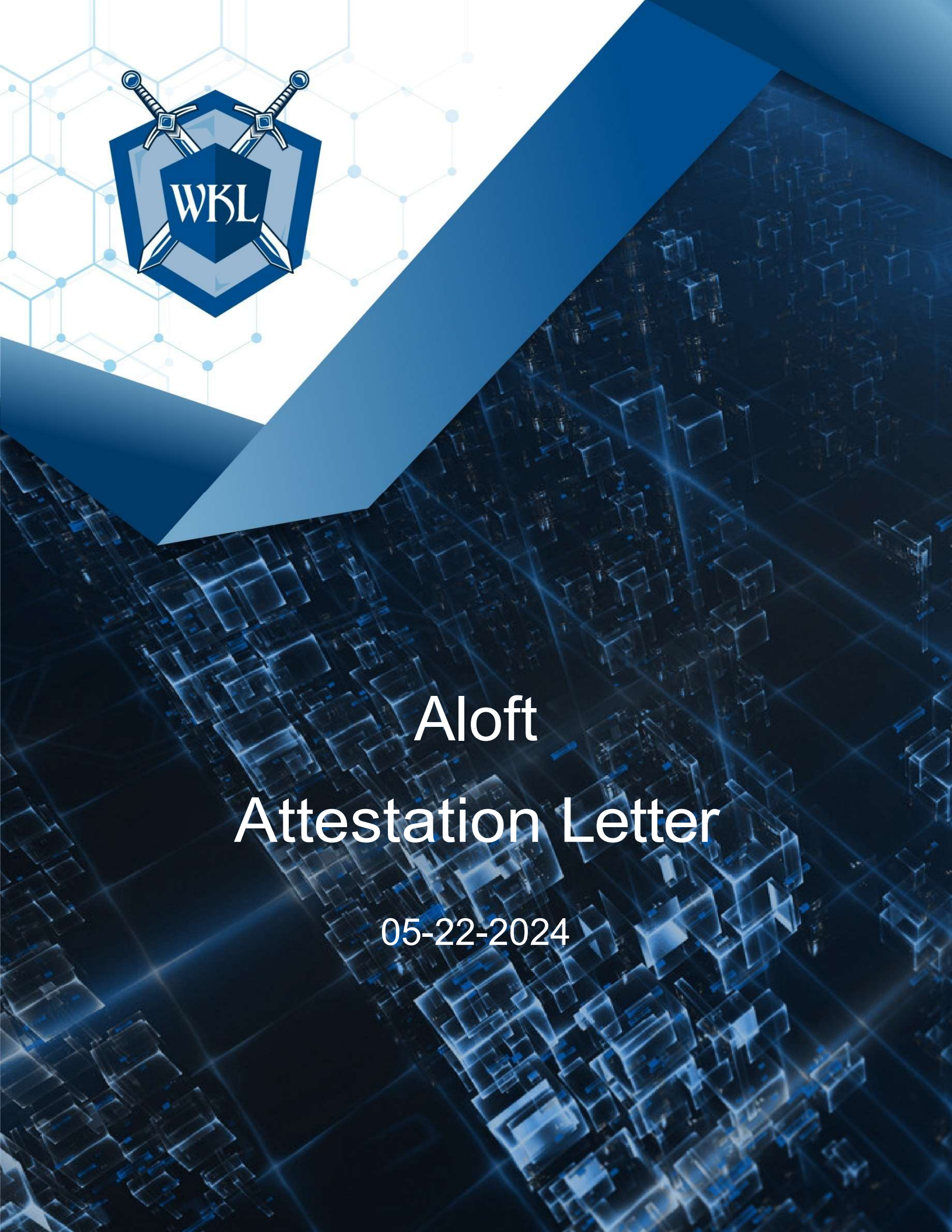

Aloft
Attestation Letter

05-22-2024

Engagement Overview

Security is a journey, not a destination. One must remain vigilant and continue to invest in and strive towards a robust security posture. The threat landscape is ever-changing and malicious actors are always innovating. As the internet becomes more hostile, defenders must enhance their capabilities as well.

White Knight Labs conducted a Web Application Penetration Test of the Aloft web application. This test was performed to evaluate the security of Aloft's web application and to proactively identify any vulnerabilities, validate their severity, and provide recommended remediation steps. Through addressing these vulnerabilities, Aloft can improve its defensive posture and better protect its sensitive information and infrastructure from potential attacks.

The testing was performed between April 24, 2024 and May 10, 2024 and represents a point-in-time look at the security posture of the in-scope domains.

Scoping and Rules of Engagement

While malicious actors have no limits on their actions, WKL understands the need to scope assessments to complete the assessment in a timely manner and protect third parties not participating in the engagement.

- **Web Application Test** – The goal of a web application penetration test is to identify vulnerabilities in a web application, evaluate the effectiveness of existing security controls, and provide recommendations for improving the security of the application. Its purpose is to improve the security posture of the application, protect against potential attacks, and safeguard sensitive information.

WKL conducted the web application penetration test in two parts:

- **Black-Box Testing** – In a black-box engagement, the consultant does not have access to any internal information and is not granted internal access to the client's applications or network. It is the job of the consultant to perform all reconnaissance to obtain the sensitive knowledge needed to proceed, which places them in a role as close to the typical attacker as possible.
- **White-Box Testing** – In a white-box engagement, the consultant is provided with all internal information, including source code, architecture diagrams, and network configurations of the client's applications or network. This comprehensive access allows the consultant to thoroughly examine the internal workings of the application or network, enabling them to identify vulnerabilities that may not be visible during a black-box test. It places the consultant in a position similar to an insider with comprehensive knowledge and access, allowing for a detailed and exhaustive analysis of the security posture from the inside out.

WKL evaluated the following URLs that provided access to the Aloft web application:

- https://air.aloft.ai
- https://api.aloft.ai

The following timeline details the entire engagement of the Aloft network:

- **Kickoff Call** – 4/2/2024
- **Engagement Testing** – 4/24/2024-5/10/2024
- **Debrief Call** – TBD

Finding Severity Summary

As a result of this engagement, White Knight Labs conducted a comprehensive assessment within the client-defined scope of the Aloft environment. The primary objective of this assessment was to identify vulnerabilities that could potentially compromise the confidentiality, integrity, and availability of Aloft's critical information assets.

During the assessment, White Knight Labs diligently examined the environment, applying rigorous testing methodologies in alignment with industry best practices. As a result, White Knight Labs identified a total of **7** findings, each of which has been carefully categorized based on its severity.

The following table provides a summary of these findings, including their respective severity levels. Detailed descriptions of each finding, along with additional information and recommendations for mitigation, are provided in subsequent sections of this report.

White Knight Labs did not find evidence of any data or traffic leaving the Aloft environment and reaching out to non-Aloft controlled endpoints or Chinese endpoints, domains, or infrastructure.

Severity definitions, essential for understanding the impact and urgency of each finding, can be found in Appendix A. ensuring clarity in assessing and addressing the identified vulnerabilities.